

# 配置9800 WLC和Aruba ClearPass — 訪客訪問和FlexConnect

## 目錄

---

### [簡介](#)

### [必要條件](#)

[需求](#)

[採用元件](#)

### [背景資訊](#)

[CWA訪客企業部署的流量流](#)

[網路圖表](#)

### [設定](#)

[配置訪客無線接入C9800引數](#)

[C9800 — 訪客的AAA組態](#)

[C9800 — 設定重新導向ACL](#)

[C9800 — 訪客WLAN設定檔設定](#)

[C9800 — 訪客原則設定檔定義](#)

[C9800 — 策略標籤](#)

[C9800 - AP加入配置檔案](#)

[C9800 — 彈性設定檔](#)

[C9800 — 站點標籤](#)

[C9800 - RF設定檔](#)

[C9800 — 為AP分配標籤](#)

[配置Aruba CPPM例項](#)

[Aruba ClearPass伺服器初始配置](#)

[申請授權](#)

[伺服器主機名](#)

[生成CPPM Web伺服器證書\(HTTPS\)](#)

[將C9800 WLC定義為網路裝置](#)

[訪客入口頁面和CoA計時器](#)

[ClearPass — 訪客CWA組態](#)

[ClearPass端點後設資料屬性：Allow-Guest-Internet](#)

[ClearPass重新驗證實施策略配置](#)

[ClearPass訪客輸入網站重新導向執行設定檔組態](#)

[ClearPass後設資料實施配置檔案配置](#)

[ClearPass Guest Internet Access Enforcement策略配置](#)

[ClearPass訪客在AUP後實施策略配置](#)

[ClearPass MAB身份驗證服務配置](#)

[ClearPass Webauth服務組態](#)

[ClearPass - Web登入](#)

[驗證 — 訪客CWA授權](#)

### [附錄](#)

### [相關資訊](#)

---

# 簡介

本檔案介紹Catalyst 9800無線LAN控制器(WLC)與Aruba ClearPass的整合，以提供訪客無線服務組識別碼(SSID)。

## 必要條件

本指南假設已配置和驗證以下元件：

- 所有相關元件均同步到網路時間協定(NTP)並驗證其時間是否正確 ( 驗證證書時需要 )
- 操作DNS伺服器(訪客流量流需要，證書吊銷清單(CRL)驗證)
- 可操作的DHCP伺服器
- 可選的證書頒發機構(CA) ( 簽署CPPM託管訪客門戶時需要 )
- Catalyst 9800 WLC
- Aruba ClearPass Server ( 需要平台許可證、訪問許可證、板載許可證 )
- Vmware ESXi

## 需求

思科建議您瞭解以下主題：

- C9800部署和新的配置模式
- C9800上的Flexconnect交換
- 9800 CWA驗證(請參閱<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213920-central-web-authentication-cwa-on-cata.html>)

## 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行17.3.4c的Cisco Catalyst C9800-L-C
- Cisco Catalyst C9130AXE
- Aruba ClearPass，6-8-0-109592和6.8-3修補程式
- MS Windows伺服器
  - Active Directory ( GP配置為向託管端點自動頒發基於電腦的證書 )
  - 帶有選項43和選項60的DHCP伺服器
  - DNS伺服器
  - NTP伺服器可對所有元件進行時間同步
  - CA

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 ( 預設 ) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

Catalyst 9800 WLC實作的整合在存取點(AP)部署的Flexconnect模式下為無線使用者端使用中央

Web驗證(CWA)。

訪客無線身份驗證由訪客門戶支援，帶有匿名可接受使用者策略(AUP)頁面，該頁面託管在Aruba Clearpass的安全隔離區(DMZ)網段中。

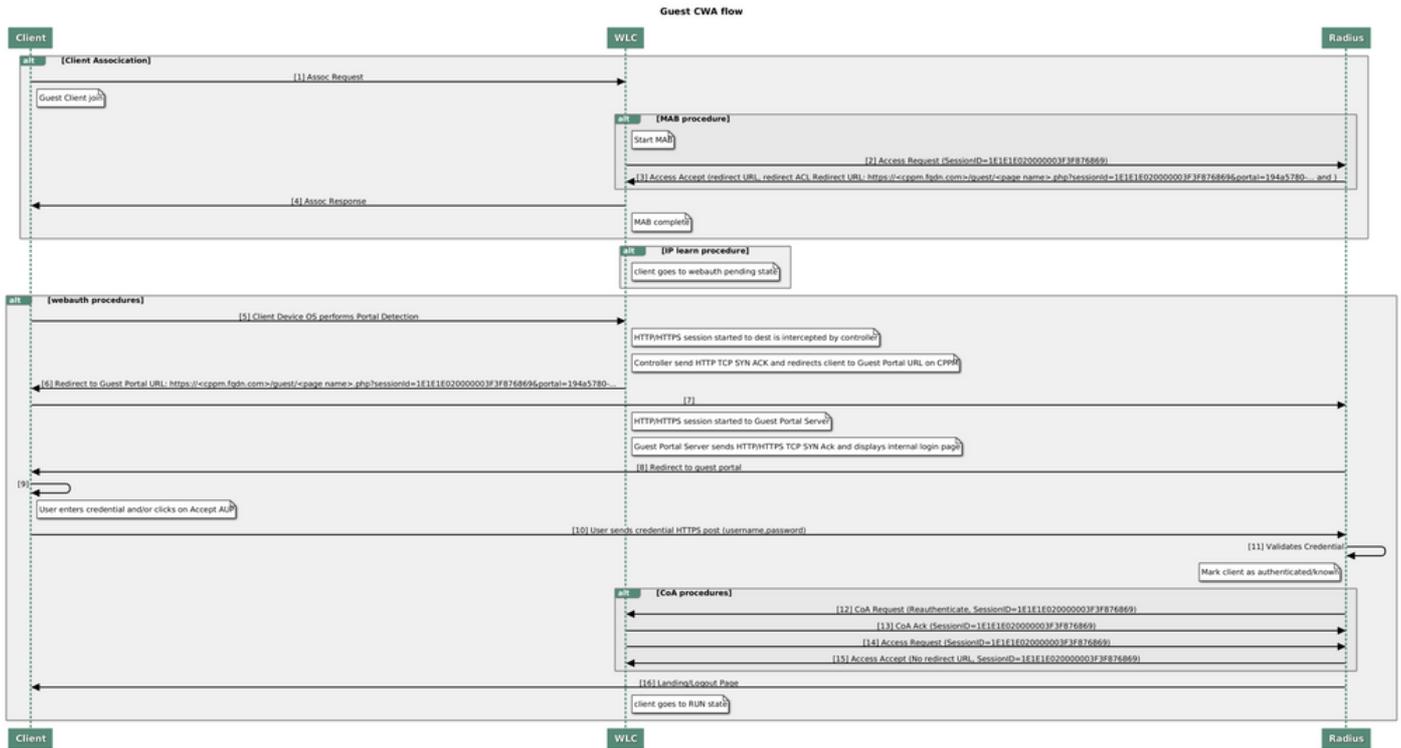
該圖顯示了訪客WiFi接入交換的詳細資訊，之後允許訪客使用者訪問網路：

- 1.訪客使用者與遠端辦公室中的訪客Wifi相關聯。
- 2.初始RADIUS訪問請求由C9800代理到RADIUS伺服器。
- 3.伺服器在本地MAC終端資料庫中查詢提供的訪客MAC地址。  
如果未找到MAC地址，則伺服器將使用MAC Authentication Bypass(MAB)配置檔案進行響應。此RADIUS響應包括：
  - URL重新導向存取控制清單(ACL)
  - URL重新導向
- 4.客戶端將通過IP Learn過程，並在該過程中為其分配IP地址。
5. C9800將訪客使用者端（由其MAC位址識別）轉換為「Web Auth Pending」狀態。
- 6.大多數與訪客WLAN關聯的現代裝置OS都會執行某種強制網路門戶檢測。  
確切的檢測機製取決於具體的作業系統實施。客戶端作業系統會開啟一個彈出視窗（偽瀏覽器）對話方塊，其中的頁面由C9800重定向到由RADIUS伺服器託管的訪客門戶URL，作為RADIUS訪問接受響應的一部分提供。
- 7.訪客使用者接受所顯示的彈出視窗中的條款和條件ClearPass在其終端資料庫(DB)中為客戶端MAC地址設定一個標誌，以指示客戶端已完成身份驗證，並通過根據路由表選擇介面（如果ClearPass上有多個介面）來啟動RADIUS授權更改(CoA)。
8. WLC將訪客使用者端轉換為「執行」狀態，且使用者被授權存取網際網路，沒有進一步的重新導向。

---

 注意：有關Cisco 9800外部、錨點無線控制器狀態流程圖以及RADIUS和外部託管訪客門戶，請參閱本文的附錄部分。

---



訪客中央Web驗證(CWA)狀態圖表

## CWA訪客企業部署的流量流

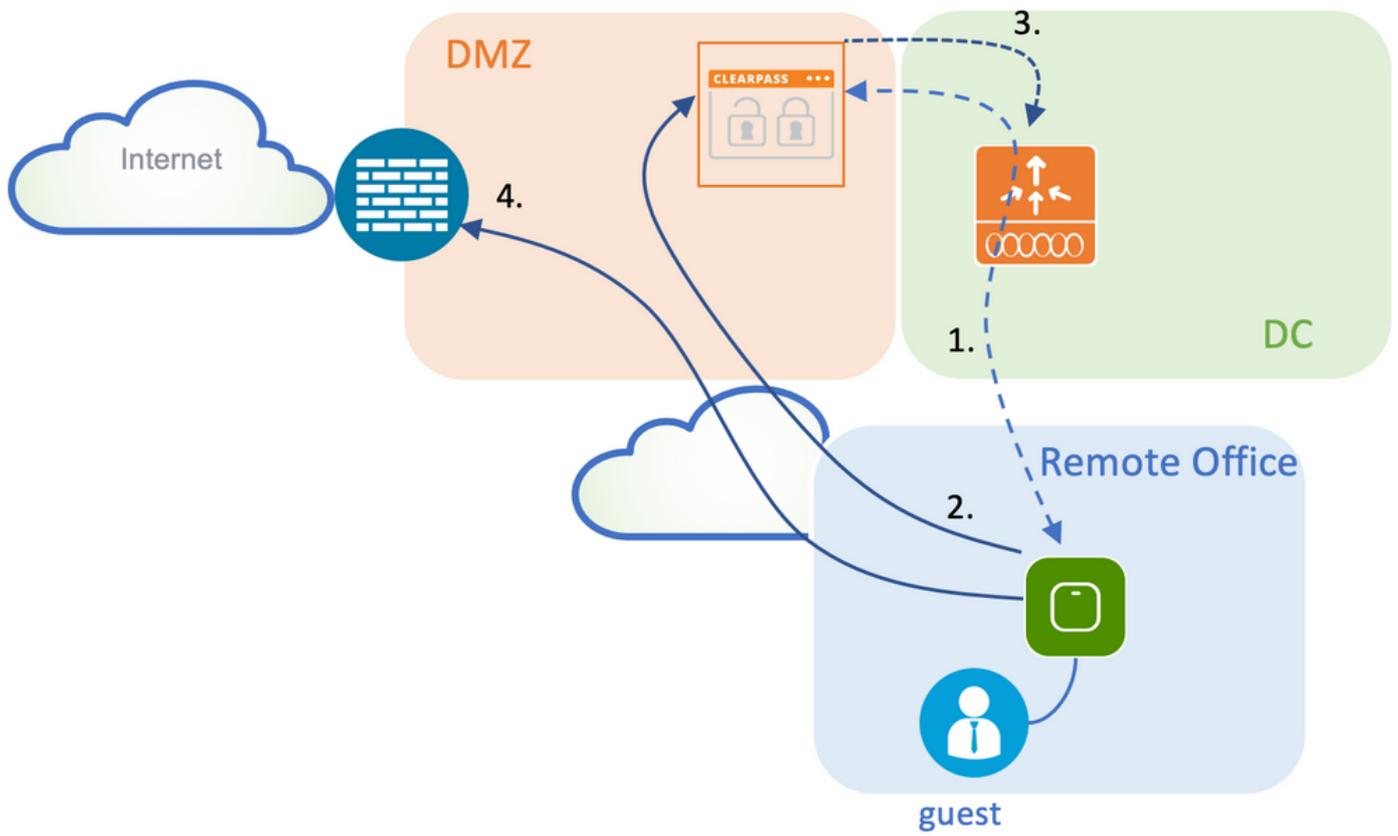
在具有多個分支機構的典型企業部署中，每個分支機構都設定為在訪客接受EULA後，通過訪客門戶提供對訪客的安全、分段訪問。

在此配置示例中，9800 CWA用於通過整合到單獨的ClearPass例項來訪問訪客，該ClearPass例項專門為網路安全DMZ中的訪客使用者部署。

訪客必須接受DMZ ClearPass伺服器提供的Web許可彈出門戶中列出的條款和條件。此配置示例重點介紹匿名訪客訪問方法（即，無需訪客使用者名稱/密碼即可對訪客門戶進行身份驗證）。

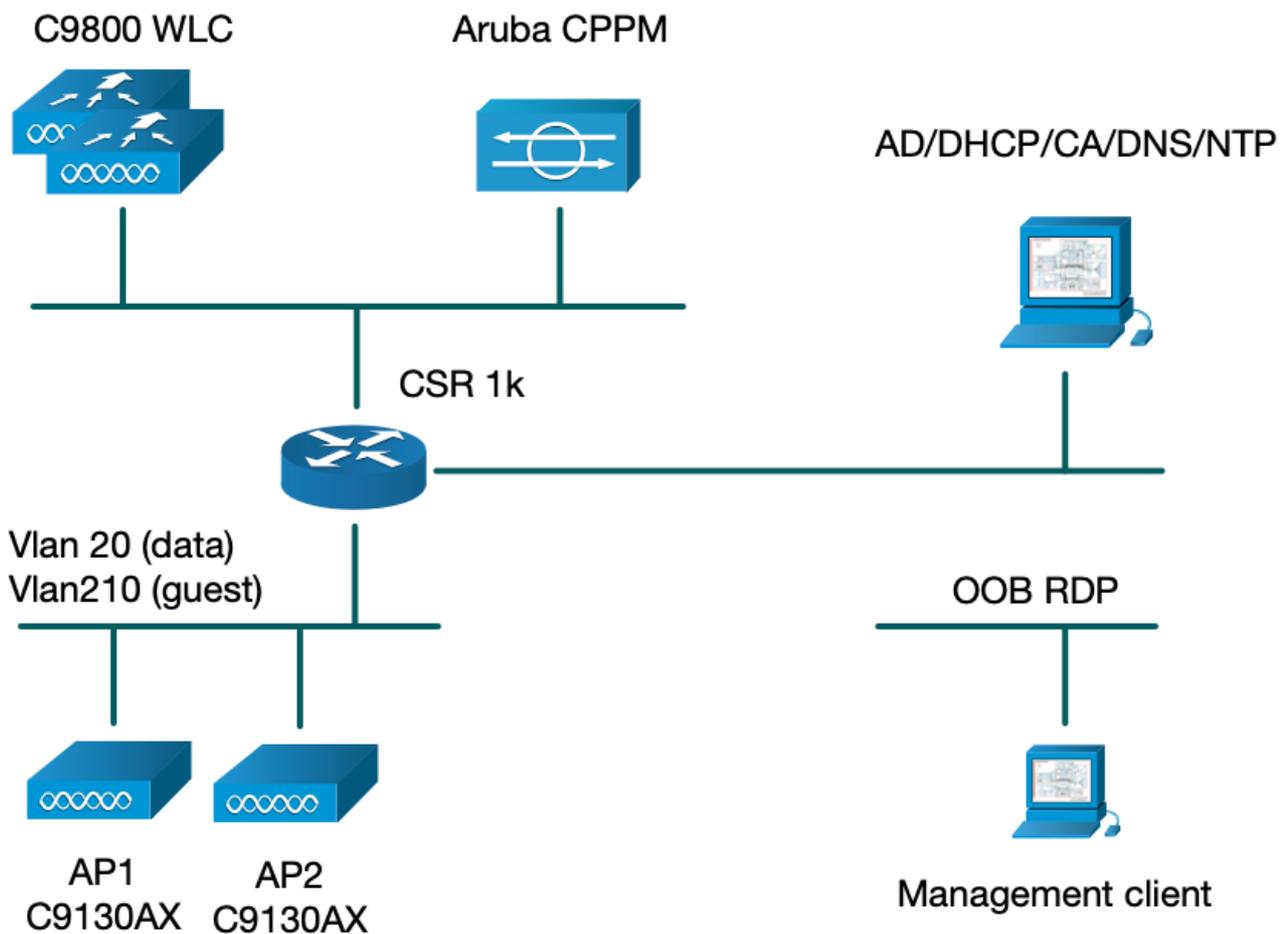
對應於此部署的流量如下圖所示：

1. RADIUS - MAB階段
2. 訪客使用者端URL重新導向到訪客輸入網站
3. 訪客在訪客入口上接受EULA後，會從CPPM向9800 WLC發出RADIUS CoA Reauthenticate
4. 允許訪客訪問網際網路



## 網路圖表

 注意：為了進行實驗室演示，使用單個/組合的Aruba CPPM伺服器例項來同時提供訪客和公司SSID網路訪問伺服器(NAS)功能。最佳做法實施建議使用獨立的NAS例項。



## 設定

在此配置示例中，利用C9800上的新配置模型來建立必要的配置檔案和標籤，以便為企業分支機構提供dot1x企業訪問和CWA訪客訪問。所得組態概述在此圖中：

AP  
MAC: XXXX.XXXX.XXXX

Policy Tag: PT\_CAN01

WLAN Profile: WP\_Guest  
SSID: Guest  
Layer 2: Security None  
Layer 2: MAC Filtering Enabled  
Authz List: AAA\_Authz-CPPM

Policy Profile: PP\_Guest  
Central Switching: Disabled  
Central Auth: Enabled  
Central DHCP: Disabled  
Vlan: guest (21)  
AAA Policy: Allow AAA Override Enabled  
AAA Policy: NAC State Enabled  
AAA Policy: NAC Type RADIUS  
AAA Policy Accounting List: Guest\_Accounting

Site Tag: ST\_CAN01  
Enable Local Site: Off

AP Join Profile: MyApProfile  
NTP Server: 10.0.10.4

Flex Profile: FP\_CAN01  
Native Vlan 2  
Policy ACL: CAPTIVE\_PORTAL\_REDIRECT,  
ACL CWA: Enabled  
VLAN: 21 (Guest)

RF Tag: Branch\_RF

5GHz Band RF: Typical\_Client\_Density\_rf\_5gh

2GHz Band RF: Typical\_Client\_Density\_rf\_2gh

## 配置訪客無線接入C9800引數

### C9800 — 訪客的AAA組態

 註：關於Cisco錯誤ID [CSCvh03827](#)，請確保定義的身份驗證、授權和記帳(AAA)伺服器未進行負載平衡，因為此機制依賴WLC中的SessionID持續性來進行ClearPass RADIUS交換。

步驟 1. 將Aruba ClearPass DMZ伺服器新增到9800 WLC配置中，並建立身份驗證方法清單。導覽至Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > +Add，然後輸入RADIUS伺服器資訊。

## Create AAA Radius Server

|                          |   |
|--------------------------|---|
| Name*                    | <input type="text" value="CPPM"/>           |
| Server Address*          | <input type="text" value="10.85.54.98"/>    |
| PAC Key                  | <input type="checkbox"/>                    |
| Key Type                 | <input type="text" value="Clear Text"/>     |
| Key* ⓘ                   | <input type="text" value="....."/>          |
| Confirm Key*             | <input type="text" value="....."/>          |
| Auth Port                | <input type="text" value="1812"/>           |
| Acct Port                | <input type="text" value="1813"/>           |
| Server Timeout (seconds) | <input type="text" value="5"/>              |
| Retry Count              | <input type="text" value="3"/>              |
| Support for CoA          | <input checked="" type="checkbox"/> ENABLED |

Cancel

Apply to Device

步驟 2. 為來賓定義AAA伺服器組，並將步驟1中配置的伺服器分配給此伺服器組。導航至 Configuration > Security > AAA > Servers/Groups > RADIUS > Groups > +Add。

## Create AAA Radius Server Group

|                          |  |
|--------------------------|--|
| Name*                    | <input type="text" value="AAA_Radius_CPPM"/> |
| Group Type               | <input type="text" value="RADIUS"/>          |
| MAC-Delimiter            | <input type="text" value="none"/>            |
| MAC-Filtering            | <input type="text" value="none"/>            |
| Dead-Time (mins)         | <input type="text" value="5"/>               |
| Source Interface VLAN ID | <input type="text" value="1"/>               |

Available Servers

Assigned Servers



CPPM



Cancel

Apply to Device

步驟 3. 為訪客訪問定義授權方法清單並對映在步驟2中建立的伺服器組。 導航至 Configuration > Security > AAA > AAA Method List > Authorization > +Add。 選擇 Type Network，然後在 AAA Server Group 步驟2中配置。

### Quick Setup: AAA Authorization

Method List Name\*

Type\*  ⓘ

Group Type  ⓘ

Fallback to local

Authenticated

Available Server Groups

- radius
- ldap
- tacacs+

Assigned Server Groups

- AAA\_Radius\_CPPM

步驟 4. 為訪客訪問建立記帳方法清單並對映在步驟2中建立的伺服器組。 導航至 Configuration > Security > AAA > AAA Method List > Accounting > +Add。 從下拉選單中選擇 Type Identity，然後在 AAA Server Group 步驟2中進行配置。

### Quick Setup: AAA Accounting

Method List Name\*

Type\*  ⓘ

Available Server Groups

- radius
- ldap
- tacacs+

Assigned Server Groups

- AAA\_Radius\_CPPM

重新導向ACL定義哪些流量必須重新導向至訪客入口網站，而哪些流量允許通過而沒有重新導向。這裡，ACL deny表示繞過重新導向或通過，而permit表示重新導向到入口網站。對於每個流量類，在建立訪問控制條目(ACE)並建立與入口和出口流量均匹配的ACE時，必須考慮流量的方向。

導覽至Configuration > Security > ACL，然後定義一個名為CAPTIVE\_PORTAL\_REDIRECT的新ACL。使用以下ACE配置ACL：

- ACE1：允許雙向網際網路控制消息協定(ICMP)流量繞過重定向，主要用於驗證可達性。
- ACE10、ACE30：允許雙向的DNS流量流到DNS伺服器10.0.10.4，並且不會重定向到門戶。觸發訪客流需要DNS查詢和偵聽響應。
- ACE70、ACE80、ACE110、ACE120：允許使用者與門戶一起訪問訪客強制網路門戶的HTTP和HTTPS訪問。
- ACE150：重定向所有HTTP流量 ( UDP埠80 )。

| Sequence ▲ | Action ▼ | Source IP ▼ | Source Wildcard ▼ | Destination IP ▼ | Destination Wildcard ▼ | Protocol ▼ | Source Port ▼ | Destination Port ▼ |
|------------|----------|-------------|-------------------|------------------|------------------------|------------|---------------|--------------------|
| 1          | deny     | any         |                   | any              |                        | icmp       |               |                    |
| 10         | deny     | any         |                   | 10.0.10.4        |                        | udp        |               | eq domain          |
| 30         | deny     | 10.0.10.4   |                   | any              |                        | udp        | eq domain     |                    |
| 70         | deny     | any         |                   | 10.85.54.98      |                        | tcp        |               | eq 443             |
| 80         | deny     | 10.85.54.98 |                   | any              |                        | tcp        | eq 443        |                    |
| 110        | deny     | any         |                   | 10.85.54.98      |                        | tcp        |               | eq www             |
| 120        | deny     | 10.85.54.98 |                   | any              |                        | tcp        | eq www        |                    |
| 150        | permit   | any         |                   | any              |                        | tcp        |               | eq www             |

## C9800 — 訪客WLAN設定檔設定

步驟 1.導航至Configuration > Tags & Profiles > Wireless > +Add。建立新的SSID配置檔案WP\_Guest，並廣播訪客客戶端關聯的SSID 'Guest'。

## Add WLAN

### General

### Security

### Advanced

|               |   |                |   |
|---------------|---|----------------|---|
| Profile Name* | <input type="text" value="WP_Guest"/>       | Radio Policy   | <input type="text" value="All"/>            |
| SSID*         | <input type="text" value="Guest"/>          | Broadcast SSID | <input checked="" type="checkbox"/> ENABLED |
| WLAN ID*      | <input type="text" value="3"/>              |                |   |
| Status        | <input checked="" type="checkbox"/> ENABLED |                |   |

Cancel

Apply to Device

在同一對話框Add WLAN下，導航到選項卡Security > Layer 2。

— 第2層安全模式：無

- MAC過濾：已啟用

— 授權清單：下拉選單中的AAA\_Authz\_CPPM ( 在步驟3下配置。作為AAA配置的一部分 )

## Add WLAN

### General

### Security

### Advanced

#### Layer2

#### Layer3

#### AAA

|                          |  |                       |   |
|--------------------------|--|-----------------------|---|
| Layer 2 Security Mode    | <input type="text" value="None"/>        | Lobby Admin Access    | <input type="checkbox"/>                      |
| MAC Filtering            | <input checked="" type="checkbox"/>      | Fast Transition       | <input type="text" value="Adaptive Enab..."/> |
| OWE Transition Mode      | <input checked="" type="checkbox"/>      | Over the DS           | <input type="checkbox"/>                      |
| Transition Mode WLAN ID* | <input type="text" value="1-4096"/>      | Reassociation Timeout | <input type="text" value="20"/>               |
| Authorization List*      | <input type="text" value="AAA_Authz_C"/> |                       |   |

Cancel

Apply to Device

## C9800 — 訪客原則設定檔定義

在C9800 WLC GUI上，導航至Configuration > Tags & Profiles > Policy > +Add。

名稱：PP\_Guest

狀態：已啟用

集中交換：已禁用

集中身份驗證：已啟用

中央DHCP：已禁用

中央關聯：已禁用

### Add Policy Profile ✕

**General** | Access Policies | QOS and AVC | Mobility | Advanced

**⚠** Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

|                             |   |                              |   |
|-----------------------------|---|------------------------------|---|
| Name*                       | <input type="text" value="PP_Guest"/>                 | <b>WLAN Switching Policy</b> |   |
| Description                 | <input type="text" value="Policy Profile for Guest"/> | Central Switching            | <input type="checkbox"/> DISABLED           |
| Status                      | <input checked="" type="checkbox"/> ENABLED           | Central Authentication       | <input checked="" type="checkbox"/> ENABLED |
| Passive Client              | <input type="checkbox"/> DISABLED                     | Central DHCP                 | <input type="checkbox"/> DISABLED           |
| Encrypted Traffic Analytics | <input type="checkbox"/> DISABLED                     | Central Association          | <input type="checkbox"/> DISABLED           |
| <b>CTS Policy</b>           |   | Flex NAT/PAT                 | <input type="checkbox"/> DISABLED           |
| Inline Tagging              | <input type="checkbox"/>                              |                              |   |
| SGACL Enforcement           | <input type="checkbox"/>                              |                              |   |
| Default SGT                 | <input type="text" value="2-65519"/>                  |                              |   |

Add Policy Profile ✕

**⚠** Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

**General**   Access Policies   QOS and AVC   Mobility   Advanced

---

Name\*

Description

Status  DISABLED

Passive Client  DISABLED

Encrypted Traffic Analytics  DISABLED

**CTS Policy**

Inline Tagging

SGACL Enforcement

Default SGT

**WLAN Switching Policy**

Central Switching  DISABLED

**Central Authentication**  **ENABLED**

Central DHCP  DISABLED

Central Association  DISABLED

Flex NAT/PAT  DISABLED

Access Policies 導航到同一對話方塊中的Add Policy Profile頁籤。

- RADIUS分析：已啟用

- VLAN/VLAN組：210 ( 即，VLAN 210是每個分支機構位置的訪客本地VLAN )

注意：在9800 WLC上的VLAN下、VLAN/VLAN組型別VLAN編號中，不得定義Flex的訪客VLAN。

已知缺陷：如果WLC和Flex配置檔案中定義了相同的Flex訪客VLAN，則思科錯誤ID [CSCvn48234](#)會導致無法廣播SSID。

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

General **Access Policies** QOS and AVC Mobility Advanced

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

#### WLAN Local Profiling

Global State of Device Classification ⓘ

Local Subscriber Policy Name

Search or Select ▼

#### VLAN

VLAN/VLAN Group

210 ▼

Multicast VLAN

Enter Multicast VLAN

#### WLAN ACL

IPv4 ACL

Search or Select ▼

IPv6 ACL

Search or Select ▼

#### URL Filters

Pre Auth

Search or Select ▼

Post Auth

Search or Select ▼

Cancel

Apply to Device

在同一對話框中Add Policy Profile，導航到選項卡Advanced。

— 允許AAA覆蓋：已啟用

- NAC狀態：已啟用

- NAC型別：RADIUS

— 記帳清單：AAA\_Accounting\_CPPM (在步驟4中定義。作為AAA配置的一部分)

⚠️ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

General Access Policies QOS and AVC Mobility **Advanced**

### WLAN Timeout

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

Guest LAN Session Timeout

### DHCP

IPv4 DHCP Required

DHCP Server IP Address

[Show more >>>](#)

### AAA Policy

Allow AAA Override

NAC State

NAC Type

Policy Name

Accounting List

Fabric Profile

mDNS Service Policy

Hotspot Server

### User Defined (Private) Network

Status

Drop Unicast

### Umbrella

Umbrella Parameter Map  [Clear](#)

Flex DHCP Option for DNS  **ENABLED**

DNS Traffic Redirect  **IGNORE**

### WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

### Air Time Fairness Policies

2.4 GHz Policy

✎ 注意：啟用C9800 WLC以接受RADIUS CoA訊息需要「網路認可控制(NAC)狀態 — 啟用」。

## C9800 — 策略標籤

在C9800 GUI上，導航至 Configuration > Tags & Profiles > Tags > Policy > +Add。

— 名稱：PT\_CAN01

— 描述：CAN01分支站點的策略標籤

在同一對話方塊中Add Policy Tag，在WLAN-POLICY MAPS下，按一下+Add，將之前建立的WLAN配置檔案對映到策略配置檔案：

- WLAN配置檔案：WP\_Guest

— 策略配置檔案：PP\_Guest

### Add Policy Tag ✕

Name\*

Description

▼ WLAN-POLICY Maps: 0

| WLAN Profile   | Policy Profile |
|--|----------------|
| ◀ 0 ▶ 10 items per page <span>No items to display</span> |                |

Map WLAN and Policy

WLAN Profile\*  Policy Profile\*

➤ RLAN-POLICY Maps: 0

## C9800 - AP加入配置檔案

在C9800 WLC GUI上，導航至 Configuration > Tags & Profiles > AP Join > +Add。

— 名稱：Branch\_AP\_Profile

- NTP伺服器：10.0.10.4 ( 請參閱實驗拓撲圖 )。這是Branch中的AP用於同步的NTP伺服器。

## Add AP Join Profile



### General

Client

CAPWAP

AP

Management

Security

ICap

QoS

Name\*

Description

LED State

LAG Mode

NTP Server

GAS AP Rate Limit

Apphost

### OfficeExtend AP Configuration

Local Access

Link Encryption

Rogue Detection

Cancel

Apply to Device

## C9800 — 彈性設定檔

配置檔案和標籤是模組化的，可以重複用於多個站點。

在FlexConnect部署的情況下，如果所有分支機構站點使用相同的VLAN ID，則您可以重複使用相同的彈性配置檔案。

步驟 1. 在C9800 WLC GUI上，導覽至Configuration > Tags & Profiles > Flex > +Add。

— 名稱：FP\_Branch

— 本徵VLAN ID:10 ( 僅當具有非預設本徵VLAN並且要具有AP管理介面時才需要 )

**Add Flex Profile** ✕

General Local Authentication Policy ACL VLAN Umbrella

Name\*  Fallback Radio Shut

Description  Flex Resilient

Native VLAN ID  ARP Caching

HTTP Proxy Port  Efficient Image Upgrade

HTTP-Proxy IP Address  OfficeExtend AP

CTS Policy Join Minimum Latency

Inline Tagging  IP Overlap

SGACL Enforcement  mDNS Flex Profile

CTS Profile Name

在同一對話Add Flex Profile中，導航到頁籤Policy ACL，然後按一下+Add。

- ACL名稱：CAPTIVE\_PORTAL\_REDIRECT

— 中央Web驗證：已啟用

在Flexconnect部署中，當重定向在AP發生而不是C9800上發生時，每個受管AP應本地下載重定向ACL。

**Add Flex Profile** ✕

General Local Authentication **Policy ACL** VLAN Umbrella

| ACL Name | Central Web Auth                    | Pre Auth URL Filter |
|----------|-------------------------------------|---------------------|
| 0        | <input checked="" type="checkbox"/> |                     |

10 items per page No items to display

ACL Name\*

Central Web Auth

Pre Auth URL Filter

在同一對話Add Flex Profile框中，導航到VLAN頁籤並按一下+Add（請參見實驗拓撲圖）。

- VLAN名稱：訪客

- VLAN Id:210

**Add Flex Profile** ✕

General   Local Authentication   Policy ACL   **VLAN**   Umbrella

+ Add   ✕ Delete

| VLAN Name                     | ID | ACL Name |
|-------------------------------|----|----------|
| <input type="checkbox"/> data | 2  |          |

◀ ▶ 1 10 items per page 1 - 1 of 1 items

VLAN Name\*

VLAN Id\*

ACL Name

✓ Save   ↶ Cancel

↶ Cancel   📄 Apply to Device

## C9800 — 站點標籤

在9800 WLC GUI上，導覽至 Configuration > Tags & Profiles > Tags > Site > Add。

 注意：為每個必須支援兩個無線SSID的遠端站點建立一個唯一的站點標籤（如所述）。

地理位置、站點標籤和Flex Profile配置之間有1-1對映。

彈性連線站點必須具有與之關聯的彈性連線配置檔案。每個Flex Connect站點最多可以有100個接入點。

— 名稱：ST\_CAN01

- AP加入配置檔案：Branch\_AP\_Profile

— 彈性配置檔案：FP\_Branch

— 啟用本地站點：已禁用

**Add Site Tag** ✕

Name\*

Description

AP Join Profile

Flex Profile

Fabric Control Plane Name

Enable Local Site

↶ Cancel   📄 Apply to Device

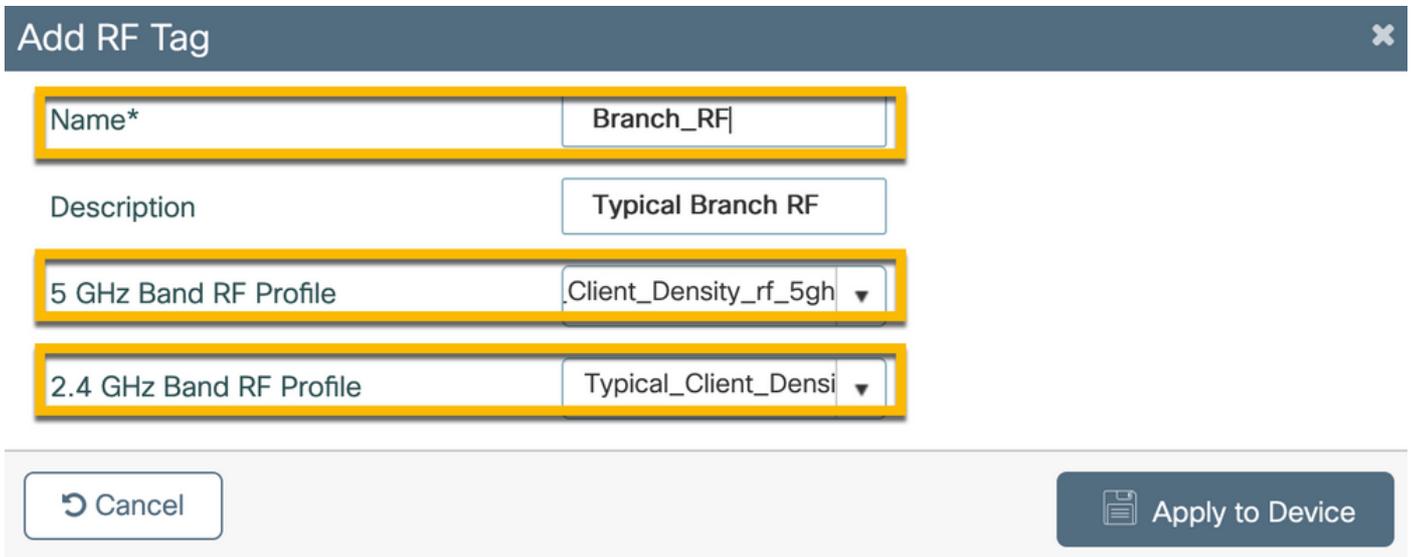
## C9800 - RF設定檔

在9800 WLC GUI上，導覽至Configuration > Tags & Profiles > Tags > RF > Add。

— 名稱：Branch\_RF

- 5 GHz頻帶射頻(RF)配置檔案：Typical\_Client\_Density\_5gh (系統定義的選項)

- 2.4 GHz頻段RF配置檔案：Typical\_Client\_Density\_2gh (系統定義的選項)



The screenshot shows the 'Add RF Tag' dialog box. The 'Name\*' field contains 'Branch\_RF'. The 'Description' field contains 'Typical Branch RF'. The '5 GHz Band RF Profile' dropdown menu is set to 'Client\_Density\_rf\_5gh'. The '2.4 GHz Band RF Profile' dropdown menu is set to 'Typical\_Client\_Densi'. The 'Cancel' button is on the left and the 'Apply to Device' button is on the right.

## C9800 — 為AP分配標籤

有兩種選項可以將定義的標籤分配給部署中的各個AP:

— 基於AP名稱的分配，利用與AP名稱欄位中的模式相匹配的regex規則(Configuration > Tags & Profiles > Tags > AP > Filter)

- AP乙太網MAC地址分配(Configuration > Tags & Profiles > Tags > AP > Static)

在使用Cisco DNA Center的生產部署中，強烈建議使用DNAC和AP PNP工作流，或使用9800中提供的靜態批次逗號分隔值(CSV)上傳方法，以避免手動分配每個AP。導覽至Configuration > Tags & Profiles > Tags > AP > Static > Add(請注意Upload File選項)。

- AP MAC地址：<AP\_ETHERNET\_MAC>

— 策略標籤名稱：PT\_CAN01

— 站點標籤名稱：ST\_CAN01

- RF標籤名稱：Branch\_RF

 註：自Cisco IOS® XE 17.3.4c起，每個控制器最多有1,000個正規表示式規則。如果部署中的站點數量超過此數量，則必須利用靜態的每MAC分配。

## Associate Tags to AP



|                 |                |
|-----------------|----------------|
| AP MAC Address* | aaaa.bbbb.cccc |
| Policy Tag Name | PT_CAN01       |
| Site Tag Name   | ST_CAN01       |
| RF Tag Name     | Branch_RF      |

Cancel

Apply to Device

注意：或者，要利用基於AP名稱正規表示式的標籤分配方法，請導航至 [Configure > Tags & Profiles > Tags > AP > Filter > Add](#)。

— 名稱：BR\_CAN01

- AP名稱正規表示式：BR-CAN01-.(7)(此規則與組織中採用的AP名稱約定匹配。在本示例中，標籤分配給具有AP名稱欄位的AP，該欄位包含「BR\_CAN01 —」，後跟任意七個字元。)

— 優先順序：1

— 策略標籤名稱：PT\_CAN01 (如定義)

— 站點標籤名稱：ST\_CAN01

- RF標籤名稱：Branch\_RF

## Associate Tags to AP



Rule "BR-CAN01" has this priority. Assigning it to the current rule will swap the priorities.

|                |   |                 |           |
|----------------|---|-----------------|-----------|
| Rule Name*     | BR_CAN01                                | Policy Tag Name | PT_CAN01  |
| AP name regex* | BR-CAN01-.{7}                           | Site Tag Name   | ST_CAN01  |
| Active         | YES <input checked="" type="checkbox"/> | RF Tag Name     | Branch_RF |
| Priority*      | 1                                       |                 |           |

Cancel

Apply to Device

配置Aruba CPPM例項

有關基於Aruba CPPM配置的生產/最佳實踐，請聯絡您當地的HPE Aruba SE資源。

### Aruba ClearPass伺服器初始配置

Aruba ClearPass使用開放式虛擬化格式(OVF)模板部署在ESXi <>伺服器上，該伺服器分配以下資源：

- 兩個保留的虛擬CPU
- 6 GB RAM
- 80 GB磁碟 ( 必須在初始虛擬機器部署後手動新增，然後才能開啟電腦 )

### 申請授權

通過申請平台許可 Administration > Server Manager > Licensing。 Add Platform、 Access和Onboard licenses。

### 伺服器主機名

導航到 Administration > Server Manager > Server Configuration，然後選擇新調配的CPPM伺服器。

— 主機名：cppm

- FQDN:cppm.example.com

— 驗證管理埠IP編址和DNS

Administration > Server Manager > Server Configuration - cppm  
Server Configuration - cppm (10.85.54.98)

The screenshot shows the 'Server Configuration' page for host 'cppm'. The 'System' tab is active. The 'Hostname' is 'cppm' and 'FQDN' is 'cppm.example.com'. Under 'Management Port', the IP Address is 10.85.54.98, Subnet Mask is 255.255.255.224, and Default Gateway is 10.85.54.97. Under 'DNS Settings', the Primary IP is 10.85.54.122. There are 'Configure' buttons for the Management Port and DNS Settings sections.

|                           | IPv4            | IPv6            | Action                    |
|---------------------------|-----------------|-----------------|---------------------------|
| <b>Management Port</b>    | IP Address      | 10.85.54.98     | <a href="#">Configure</a> |
|                           | Subnet Mask     | 255.255.255.224 |                           |
|                           | Default Gateway | 10.85.54.97     |                           |
| <b>Data/External Port</b> | IP Address      |                 | <a href="#">Configure</a> |
|                           | Subnet Mask     |                 |                           |
|                           | Default Gateway |                 |                           |
| <b>DNS Settings</b>       | Primary         | 10.85.54.122    | <a href="#">Configure</a> |
|                           | Secondary       |                 |                           |
|                           | Tertiary        |                 |                           |
|                           | DNS Caching     | Disabled        |                           |

### 生成CPPM Web伺服器證書(HTTPS)

當ClearPass Guest Portal頁面通過HTTPS呈現給連線到分支機構中訪客Wifi的訪客客戶端時，使用此證書。

步驟 1.上傳CApub chain證書。

導航至Administration > Certificates > Trust List > Add。

— 用法：啟用其他

### View Certificate Details

|                      |  |
|----------------------|--|
| Subject DN:          |  |
| Issuer DN:           |  |
| Issue Date/Time:     | Dec 23, 2020 16:55:10 EST  |
| Expiry Date/Time:    | Dec 24, 2025 17:05:10 EST  |
| Validity Status:     | Valid  |
| Signature Algorithm: | SHA256WithRSAEncryption  |
| Public Key Format:   | X.509  |
| Serial Number:       | 86452691282006080280068723651711271611   |
| Enabled:             | true   |
| Usage:               | <input checked="" type="checkbox"/> EAP <input checked="" type="checkbox"/> RadSec <input checked="" type="checkbox"/> Database <input checked="" type="checkbox"/> Others |

步驟 2. 建立證書簽名請求。

導航至Administration > Certificates > Certificate Store > Server Certificates > Usage: HTTPS Server Certificate。

— 按一下 Create Certificate Signing Request

— 通用名稱：CPPM

— 組織：cppm.example.com

確保填充SAN欄位（SAN中必須存在公用名稱，IP和其他FQDN必須根據需要存在）。格式為DNS

,DNS:

.IP

o

| Create Certificate Signing Request |                      |
|------------------------------------|----------------------|
| Common Name (CN):                  | cppm                 |
| Organization (O):                  | Cisco                |
| Organizational Unit (OU):          | Engineering          |
| Location (L):                      | Toronto              |
| State (ST):                        | ON                   |
| Country (C):                       | CA                   |
| Subject Alternate Name (SAN):      | DNS:cppm.example.com |
| Private Key Password:              | .....                |
| Verify Private Key Password:       | .....                |
| Private Key Type:                  | 2048-bit RSA v       |
| Digest Algorithm:                  | SHA-512 v            |
| <b>Submit</b> <b>Cancel</b>        |                      |

步驟 3. 在您選擇的CA中，簽署新產生的CPPM HTTPS服務CSR。

步驟 4. 導航至 Certificate Template > Web Server > Import Certificate。

— 證書型別：伺服器證書

— 用法：HTTP伺服器證書

— 證書檔案：瀏覽並選擇CA簽名的CPPM HTTPS服務證書

|                   |  |
|-------------------|--|
| Certificate Type: | Server Certificate                           |
| Server:           | cppm   |
| Usage:            | HTTPS Server Certificate                     |
| Upload Method:    | Upload Certificate and Use Saved Private Key |
| Certificate File: | Browse... No file selected.                  |

將C9800 WLC定義為網路裝置

導航至 Configuration > Network > Devices > Add。

— 名稱：WLC\_9800\_Branch

- IP或子網地址：10.85.54.99 (請參閱實驗拓撲圖)

- RADIUS共用思科：<WLC RADIUS密碼>

— 供應商名稱：Cisco

— 啟用RADIUS動態授權：1700

| Device                               | SNMP Read Settings   | SNMP Write Settings | CLI Settings | OnConnect Enforcement | Attributes |
|--------------------------------------|--|---------------------|--------------|-----------------------|------------|
| Name:                                | WLC_9800_Branch  |                     |              |                       |            |
| IP or Subnet Address:                | 10.85.54.99 (e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20) |                     |              |                       |            |
| Description:                         | Cisco 9800 WLC for Branch Guest Wifi                                 |                     |              |                       |            |
| RADIUS Shared Secret:                | .....  | Verify:             | .....        |                       |            |
| TACACS+ Shared Secret:               |  | Verify:             |              |                       |            |
| Vendor Name:                         | Cisco  |                     |              |                       |            |
| Enable RADIUS Dynamic Authorization: | <input checked="" type="checkbox"/> Port: 1700                       |                     |              |                       |            |
| Enable RadSec:                       | <input type="checkbox"/>   |                     |              |                       |            |

## 訪客入口頁面和CoA計時器

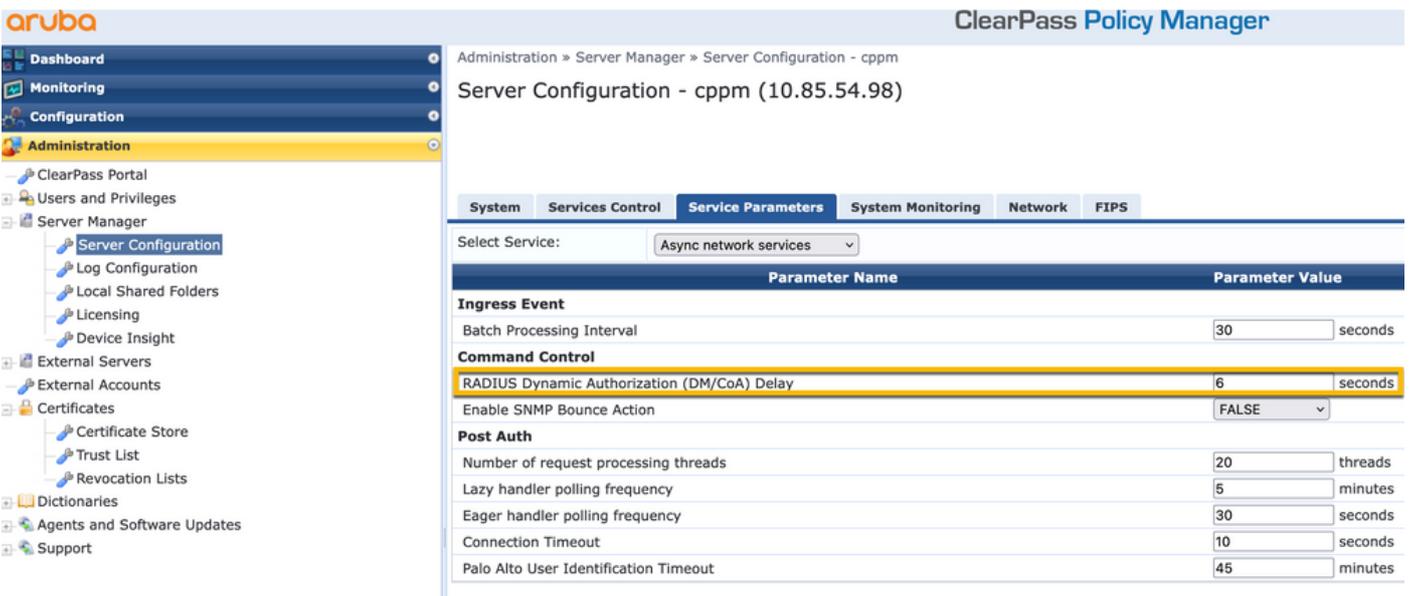
在整個配置中設定正確的計時器值非常重要。如果未調整計時器，則您可能會與客戶端一起運行循環Web門戶重定向，而不是以「運行狀態」運行。

要關注的計時器：

- 門戶Web登入計時器：此計時器將延遲您的重定向頁面，然後才允許訪問訪客門戶頁面通知CPPM服務狀態轉換、註冊終端自定義屬性「Allow-Guest-Internet」值，以及觸發從CPPM到WLC的CoA進程。導航至Guest > Configuration > Pages > Web Logins。
  - 選擇Guest Portal Name: Lab Anonymous Guest Registration (此訪客門戶頁面配置如圖所示)
  - 按一下 Edit
  - 登入延遲：6秒



- ClearPass CoA延遲計時器：這會延遲CoA訊息從ClearPass傳送到WLC的產生。在CoA確認(ACK)從WLC傳回之前，CPPM要在內部成功轉換客戶端端點的狀態，必須執行此操作。實驗室測試顯示來自WLC的次毫秒響應時間，如果CPPM尚未完成終端屬性的更新，則會將來自WLC的新RADIUS會話與未經驗證的MAB服務實施策略相匹配，然後再次向客戶端提供重定向頁面。導覽至CPPM > Administration > Server Manager > Server Configuration，然後選擇CPPM Server > Service Parameters。
  - RADIUS動態授權(DM/CoA)延遲 — 設為六秒



## ClearPass — 訪客CWA組態

ClearPass-side CWA配置由(3)服務點/階段組成：

| ClearPass元件 | 服務型別       | 目的   |
|-------------|------------|--|
| 1.策略管理器     | 服務：Mac身份驗證 | 如果自定義屬性Allow-Guest-Internet=TRUE，則允許它進入網路。否則，觸發Redirect和COA: Reauthenticate。 |

|         |               |  |
|---------|---------------|--|
| 2.訪客    | Web登入         | 顯示Anonymous login AUP頁面。<br>身份驗證後設定自定義屬性Allow-Guest-Internet= TRUE。                      |
| 3.策略管理器 | 服務：基於Web的身份驗證 | 將終端更新到 <small>Known</small><br>設定自定義屬性Allow-Guest-Internet性= TRUE<br>COA: Reauthenticate |

ClearPass端點後設資料屬性：Allow-Guest-Internet

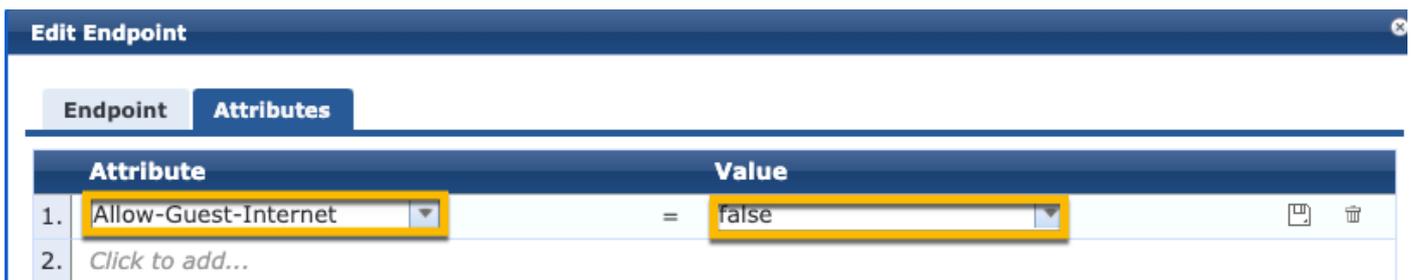
建立型別為Boolean的後設資料屬性，以便在客戶端在「Webauth Pending」和「Run」狀態之間轉換時跟蹤訪客終結點狀態：

— 連線到Wifi的新訪客具有預設後設資料屬性設定，以便Allow-Guest-Internet=false。根據此屬性，客戶端身份驗證會通過MAB服務

— 當您按一下AUP Accept按鈕時，會更新其後設資料屬性，以便Allow-Guest-Internet=true。基於此屬性的後續MAB設定為True，允許非重定向訪問Internet

導航到ClearPass > Configuration > Endpoints，從清單中選擇任何端點，按一下Attributes頁籤，Allow-Guest-Internet新增值並falseSave。

 注意：您還可以編輯同一終結點，並在之後立即刪除此屬性 — 此步驟只是在Endpoints後設資料DB中建立一個可在策略中使用的欄位。



The screenshot shows the 'Edit Endpoint' window with the 'Attributes' tab selected. It displays a table with two columns: 'Attribute' and 'Value'. The first row shows 'Allow-Guest-Internet' with a value of 'false'. The second row is a placeholder 'Click to add...'. There are also icons for adding and deleting attributes.

| Attribute               | Value   |
|-------------------------|---------|
| 1. Allow-Guest-Internet | = false |
| 2. Click to add...      |         |

ClearPass重新驗證實施策略配置

在客戶端接受Guest Portal頁面上的AUP後，立即建立分配給訪客客戶端的強制配置檔案。

導航至ClearPass > Configuration > Profiles > Add。

— 模板：RADIUS動態授權

— 名稱：Cisco\_WLC\_Guest\_COA

## Enforcement Profiles

| Profile            | Attributes  | Summary |
|--------------------|---|---------|
| Template:          | RADIUS Dynamic Authorization  |         |
| Name:              | Cisco_WLC_Guest_COA   |         |
| Description:       |   |         |
| Type:              | RADIUS_CoA  |         |
| Action:            | <input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Drop   |         |
| Device Group List: | <div style="display: flex; align-items: center;"> <div style="border: 1px solid #ccc; width: 300px; height: 40px; margin-right: 10px;"></div> <div style="display: flex; flex-direction: column; gap: 5px;"> <div style="border: 1px solid #ccc; padding: 2px 10px; background-color: #f0f0f0;">Remove</div> <div style="border: 1px solid #ccc; padding: 2px 10px; background-color: #f0f0f0;">View Details</div> <div style="border: 1px solid #ccc; padding: 2px 10px; background-color: #f0f0f0;">Modify</div> </div> </div> <div style="margin-top: 5px;"> <div style="border: 1px solid #ccc; padding: 2px 10px; background-color: #f0f0f0; display: inline-block;">--Select--</div> </div> |         |

|             |                    |  |
|-------------|--------------------|--|
| Radius:IETF | Calling-Station-Id | %{Radius:IETF:Calling-Station-Id}                        |
| Radius : 思科 | Cisco-AVPair       | subscriber:command=reauthenticate                        |
| Radius : 思科 | Cisco-AVPair       | %{Radius:Cisco:Cisco-AVPair:subscriber:audit-session-id} |
| Radius : 思科 | Cisco-AVPair       | subscriber:reauthenticate-type=last-type=last            |

### ClearPass訪客輸入網站重新導向執行設定檔組態

建立在初始MAB階段 ( 在「Allow-Guest-Internet」設定為「true」的CPPM終端資料庫中找不到MAC地址時 ) 應用於訪客的強制配置檔案。

這會導致9800 WLC將訪客使用者端重新導向到CPPM訪客輸入網站，以進行外部驗證。

導航至 [ClearPass > Enforcement > Profiles > Add](#)。

— 名稱 : Cisco\_Portal\_Redirect

— 型別 : RADIUS

— 操作：接受

Configuration » Enforcement » Profiles » Add Enforcement Profile

## Enforcement Profiles

| Profile            | Attributes  | Summary   |
|--------------------|---|---|
| Template:          | Aruba RADIUS Enforcement  |   |
| Name:              | Cisco_Portal_Redirect   |   |
| Description:       |   |   |
| Type:              | RADIUS  |   |
| Action:            | <input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Drop |   |
| Device Group List: |   | <div style="text-align: right;"><button>Remove</button><br/><button>View Details</button><br/><button>Modify</button></div> |
|                    |   | --Select--  |

ClearPass重新導向執行設定檔

在同一對話方塊中，在Attributes頁籤下，根據此影象配置兩個屬性：

Enforcement Profiles - Cisco\_Portal\_Redirect

| Summary          | Profile      | Attributes   |
|------------------|--------------|--|
| Type             | Name         | Value  |
| 1. Radius: Cisco | Cisco-AVPair | = url-redirect-acl=CAPTIVE_PORTAL_REDIRECT   |
| 2. Radius: Cisco | Cisco-AVPair | = url-redirect=https://cppm.example.com/guest/iaccept.php?cmd-login&mac=%{Connection:Client-Mac-Address-Hyphen}&switchip=%{Radius:IETF:NAS-IP-Address} |

ClearPass重新導向設定檔屬性

url-redirect-acl attribute設定為CAPTIVE-PORTAL-REDIRECT，是在C9800上建立的ACL的名稱。

 註：RADIUS消息中只傳遞對ACL的引用，而不傳遞ACL內容。在9800 WLC上建立的ACL名稱必須完全符合此RADIUS屬性的值，如圖所示。

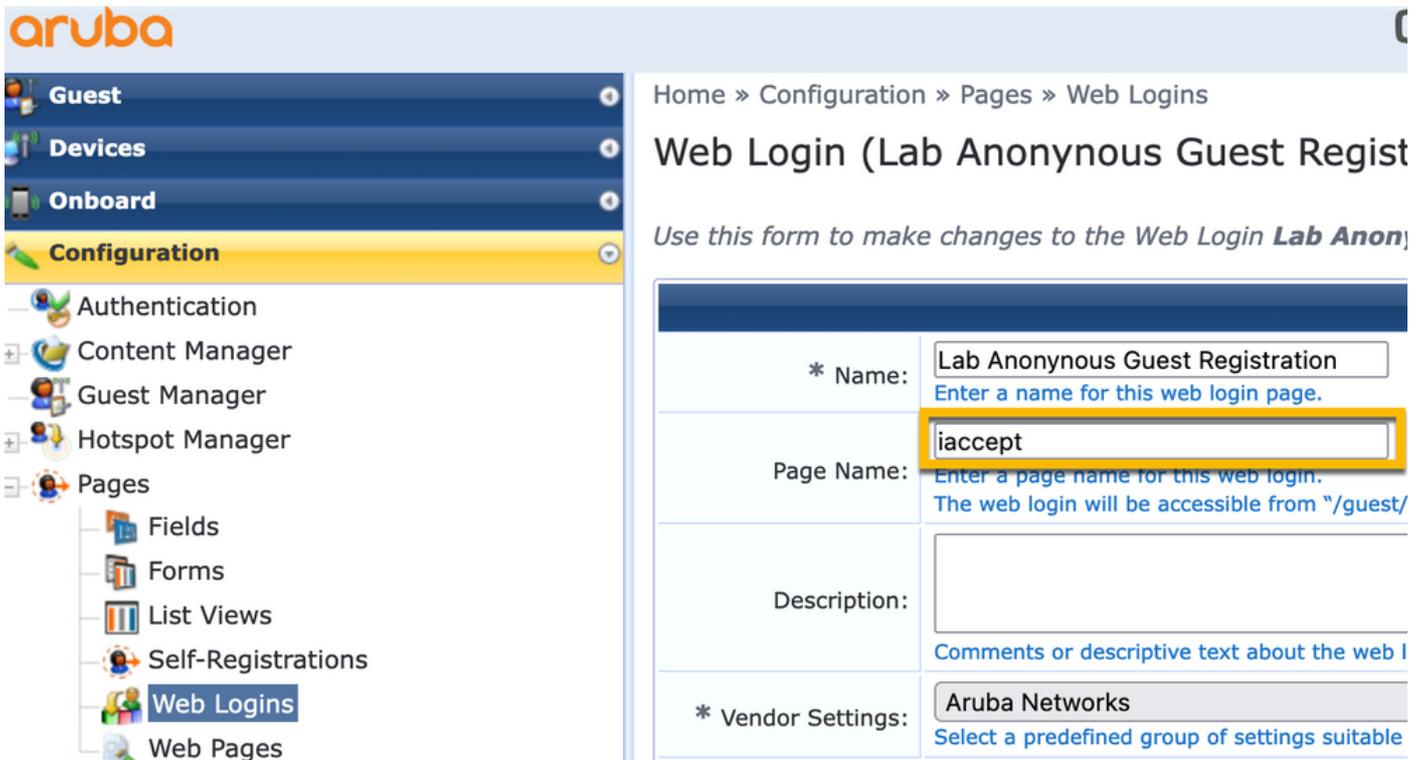
url-redirect屬性由多個參陣列成：

- 託管訪客門戶的目標URL，<https://cppm.example.com/guest/iaccept.php>
- 訪客客戶端MAC，宏%{Connection:Client-Mac-Address-Hyphen}
- 驗證器IP（9800 WLC觸發重定向），宏%{Radius:IETF:NAS-IP-Address}
- cmd-login操作

當您導航到CPPM > Guest > Configuration > Pages > Web Logins > Edit時，會看到ClearPass Guest Web Login Page的URL。

在本示例中，CPPM中的Guest Portal頁面名稱定義為iaccept。

 註:Guest Portal頁面的配置步驟如下所述。



Home » Configuration » Pages » Web Logins

### Web Login (Lab Anonymous Guest Registration)

Use this form to make changes to the Web Login **Lab Anonymous Guest Registration**.

|                    |  |
|--------------------|--|
| * Name:            | Lab Anonymous Guest Registration<br><small>Enter a name for this web login page.</small>                           |
| Page Name:         | iaccept<br><small>Enter a page name for this web login.<br/>The web login will be accessible from "/guest/</small> |
| Description:       | <br><small>Comments or descriptive text about the web login</small>  |
| * Vendor Settings: | Aruba Networks<br><small>Select a predefined group of settings suitable</small>                                    |

 註：對於思科裝置，通常使用audit\_session\_id，但其他供應商不支援此功能。

## ClearPass後設資料實施配置檔案配置

配置實施配置檔案以更新用於由CPPM跟蹤狀態轉換的終結點後設資料屬性。

此配置檔案應用於終端資料庫中訪客客戶端的MAC地址條目，並將參數Allow-Guest-Internet設定為「true」。

導航至ClearPass > Enforcement > Profiles > Add。

— 模板：ClearPass實體更新實施

— 型別：Post\_Authentication

## Enforcement Profiles

| Profile            | Attributes  | Summary   |
|--------------------|---|---|
| Template:          | ClearPass Entity Update Enforcement   |   |
| Name:              | Make-Cisco-Guest-Valid  |   |
| Description:       |   |   |
| Type:              | Post_Authentication   |   |
| Action:            | <input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Drop |   |
| Device Group List: | <input type="text"/><br><input type="text"/><br><input type="text"/>                            | <input type="button" value="Remove"/><br><input type="button" value="View Details"/><br><input type="button" value="Modify"/> |

在同一對話方塊中，選擇Attributes頁籤。

— 型別：終結點

— 名稱：Allow-Guest-Internet

 注意：要將此名稱顯示在下拉選單中，必須至少為一個「終結點」手動定義此欄位，如步驟中所述。

— 值：true

## Enforcement Profiles

| Profile            | Attributes           | Summary |
|--------------------|----------------------|---------|
| Type               | Name                 | Value   |
| 1. Endpoint        | Allow-Guest-Internet | = true  |
| 2. Click to add... |                      |         |

### ClearPass Guest Internet Access Enforcement策略配置

導航至ClearPass > Enforcement > Policies > Add。

— 名稱：WLC Cisco Guest Allow

— 實施型別：RADIUS

— 預設配置檔案：Cisco\_Portal\_Redirect

Configuration » Enforcement » Policies » Add

## Enforcement Policies

**Enforcement** Rules Summary

Name: WLC Cisco Guest Allow

Description:

Enforcement Type:  RADIUS  TACACS+  WEBAUTH (SNMP/Agent/CLI/CoA)  Application  Event

Default Profile: Cisco\_Portal\_Redirect **View Details** **Modify**

在同一對話方塊中，導航到頁籤Rules，然後按一下Add Rule。

— 型別：終結點

— 名稱：Allow-Guest-Internet

— 運算子：等於

— 值為True

— 配置檔名稱/選擇新增：[RADIUS] [允許訪問配置檔案]

Rules Editor

Conditions

Match ALL of the following conditions:

| Type               | Name                 | Operator | Value |
|--------------------|----------------------|----------|-------|
| 1. Endpoint        | Allow-Guest-Internet | EQUALS   | true  |
| 2. Click to add... |                      |          |       |

Enforcement Profiles

Profile Names: [RADIUS] [Allow Access Profile] Move Up ↑ Move Down ↓ Remove

--Select to Add--

**Save** **Cancel**

## ClearPass訪客在AUP後實施策略配置

導航至ClearPass > Enforcement > Policies > Add。

— 名稱：Cisco WLC Webauth實施策略

— 實施型別：WEBAUTH(SNMP/Agent/CLI/CoA)

— 預設配置檔案：[RADIUS\_CoA] Cisco\_Reauthenticate\_Session

## Enforcement Policies

| Enforcement       | Rules  | Summary   |
|-------------------|--|---|
| Name:             | Cisco WLC Webauth Enforcement Policy   |   |
| Description:      |  |   |
| Enforcement Type: | <input type="radio"/> RADIUS <input type="radio"/> TACACS+ <input checked="" type="radio"/> WEBAUTH (SNMP/Agent/CLI/CoA) <input type="radio"/> Application <input type="radio"/> Event |   |
| Default Profile:  | [RADIUS_CoA] Cisco_Reaut   | <input type="button" value="View Details"/> <input type="button" value="Modify"/> |

在同一對話方塊中，導航至 Rules > Add。

— 條件：身份驗證

— 名稱：狀態

— 運算子：等於

— 值：使用者

— 配置檔名稱：<add each>:

- [Post Authentication] [更新端點已知]
- [Post Authentication] [Make-Cisco-Guest-Valid]
- [RADIUS\_CoA] [Cisco\_WLC\_Guest\_COA]

**Rules Editor**

**Conditions**

Match ALL of the following conditions:

| Type               | Name   | Operator | Value |
|--------------------|--------|----------|-------|
| 1. Authentication  | Status | EQUALS   | User  |
| 2. Click to add... |        |          |       |

**Enforcement Profiles**

|                |   |   |
|----------------|---|---|
| Profile Names: | [Post Authentication] [Update Endpoint Known]<br>[Post Authentication] Make-Cisco-Guest-Valid<br>[RADIUS_CoA] Cisco_WLC_Guest_COA | <input type="button" value="Move Up ↑"/><br><input type="button" value="Move Down ↓"/><br><input type="button" value="Remove"/> |
|                | <input type="text" value="--Select to Add--"/>  |   |

註：如果遇到具有連續訪客門戶重定向偽瀏覽器彈出視窗的情況，則表明CPPM計時器需要調整或RADIUS CoA消息在CPPM和9800 WLC之間沒有正確交換。驗證這些站點。

— 導航到 CPPM > Monitoring > Live Monitoring > Access Tracker，確保RADIUS日誌條目包含RADIUS CoA詳細資訊。

— 開啟 9800 WLC Troubleshooting > Packet Capture，導航到，在預期會到達RADIUS CoA資料包的介面上啟用

PCAP，並驗證是否從CPPM收到RADIUS CoA消息。

## ClearPass MAB身份驗證服務配置

服務在屬性值(AV)配對Radius: Cisco上匹配 | CiscoAVPair | cisco-wlan-ssid

導航至ClearPass > Configuration > Services > Add。

「服務」頁籤：

— 名稱：GuestPortal - Mac Auth

— 型別：MAC身份驗證

— 更多選項：選擇授權，配置檔案終端

新增匹配規則：

— 型別：Radius: Cisco

— 名稱：Cisco-AVPair

— 運算子：等於

— 值：cisco-wlan-ssid=Guest ( 匹配配置的訪客SSID名稱 )

 註：「Guest」是由9800 WLC廣播的訪客SSID的名稱。

Configuration » Services » Add

### Services

Service Authentication Authorization Roles Enforcement Profiler Summary

Type:

Name:

Description:

Monitor Mode:  Enable to monitor network access without enforcement

More Options:  Authorization  Audit End-hosts  Profile Endpoints  Accounting Proxy

Service Rule

Matches  ANY or  ALL of the following conditions:

|    | Type         | Name               | Operator   | Value                               |   |   |
|----|--------------|--------------------|------------|-------------------------------------|---|---|
| 1. | Radius:IETF  | NAS-Port-Type      | BELONGS_TO | Ethernet (15), Wireless-802.11 (19) |  |  |
| 2. | Radius:IETF  | Service-Type       | BELONGS_TO | Login-User (1), Call-Check (10)     |  |  |
| 3. | Connection   | Client-Mac-Address | EQUALS     | %{Radius:IETF:User-Name}            |  |  |
| 4. | Radius:Cisco | Cisco-AVPair       | EQUALS     | cisco-wlan-ssid=Guest               |  |  |

在同一對話方塊中，選擇Authentication「頁籤」。

— 身份驗證方法：刪除[MAC AUTH]，新增[允許所有MAC AUTH]

— 身份驗證源：[端點儲存庫][本地SQL資料庫],[訪客使用者儲存庫][本地SQL資料庫]

Configuration » Services » Edit - GuestPortal - Mac Auth

Services - GuestPortal - Mac Auth

Summary Service **Authentication** Authorization Roles Enforcement Profiler

Authentication Methods: [Allow All MAC AUTH]

Authentication Sources: [Endpoints Repository] [Local SQL DB]  
[Guest User Repository] [Local SQL DB]

Strip Username Rules:  Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

在同一對話方塊中，選擇 Enforcement 「頁籤」。

— 實施策略：WLC Cisco Guest Allow

Configuration » Services » Add

## Services

Service Authentication Roles **Enforcement** Summary

Use Cached Results:  Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: WLC Cisco Guest Allow **Modify**

**Enforcement Policy Details**

Description: MAB Enforcement Redirect

Default Profile: Cisco\_Portal\_Redirect

Rules Evaluation Algorithm: first-applicable

| Conditions                                     | Enforcement Profiles   |
|--|------------------------|
| 1. (Endpoint:Allow-Guest-Internet EQUALS true) | [Allow Access Profile] |

在同一對話方塊中，選擇 Enforcement 「頁籤」。

## Services

| Service                  | Authentication   | Authorization | Roles | Enforcement | Profiler                | Summary                 |
|--------------------------|--|---------------|-------|-------------|-------------------------|-------------------------|
| Endpoint Classification: | Select the classification(s) after which an action must be triggered - |               |       |             |                         |                         |
|                          | <div style="border: 1px solid #ccc; height: 40px;"></div>              |               |       |             |                         | <button>Remove</button> |
|                          | -- Select --   |               |       |             |                         | ▼                       |
| RADIUS CoA Action:       | Cisco_Reauthenticate_Session   |               |       |             |                         | ▼                       |
|                          | <button>View Details</button>  |               |       |             | <button>Modify</button> |                         |

### ClearPass Webauth服務組態

導航至 ClearPass > Enforcement > Policies > Add。

— 名稱：Guest\_Portal\_Webauth

— 型別：基於Web的身份驗證

## Services

| Service  | Authentication   | Roles     | Enforcement | Summary |
|--|--|-----------|-------------|---------|
| Type:  | Web-based Authentication   |           |             |         |
| Name:  | Guest  |           |             |         |
| Description:   | <div style="border: 1px solid #ccc; height: 40px;"></div>                          |           |             |         |
| Monitor Mode:  | <input type="checkbox"/> Enable to monitor network access without enforcement      |           |             |         |
| More Options:  | <input type="checkbox"/> Authorization <input type="checkbox"/> Posture Compliance |           |             |         |
| Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions: |  |           |             |         |
| Type   | Name   |           |             |         |
| 1.   | Host   | CheckType |             |         |
| 2.   | <i>Click to add...</i>   |           |             |         |

在同一對話方塊的 Enforcement 頁籤下，Enforcement Policy: Cisco WLC Webauth Enforcement Policy。

## Services

| Service   | Authentication  | Roles                                | Enforcement | Summary                  |
|---|---|--------------------------------------|-------------|--------------------------|
| Use Cached Results: <input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions |   |                                      |             |                          |
| Enforcement Policy:   |   | Cisco WLC Webauth Enforcement Policy | Modify      | Add New Enforcement Poli |
| Enforcement Policy Details  |   |                                      |             |                          |
| Description:  |   |                                      |             |                          |
| Default Profile:  | Cisco_Reauthenticate_Session  |                                      |             |                          |
| Rules Evaluation Algorithm:   | first-applicable  |                                      |             |                          |
| Conditions  | Enforcement Profiles  |                                      |             |                          |
| 1. (Authentication:Status EQUALS User)  | [Update Endpoint Known], Make-Cisco-Guest-Valid, Cisco_Reauthenticate_Session |                                      |             |                          |

## ClearPass - Web登入

對於Anonymous AUP Guest Portal頁面，使用不帶密碼欄位的單個使用者名稱。

使用的使用者名稱必須定義/設定以下欄位：

username\_auth | 使用者名稱身份驗證：| 1

為了為使用者設定「username\_auth」欄位，該欄位必須首先在「edit user」表單中顯示。導航到 ClearPass > Guest > Configuration > Pages > Forms，然後選擇 create\_user 窗體。

The screenshot shows the ClearPass Guest configuration interface. The left sidebar contains a navigation menu with 'Forms' highlighted. The main content area displays a list of forms with columns for 'Name' and 'Title'. The 'create\_user' form is selected, and the 'Edit Fields' button is highlighted.

| Name   | Title                            |
|--|----------------------------------|
| change_expiration<br>Change the expiration time of a single guest account. | Change Expiration                |
| create_multi<br>Create multiple guest accounts.                            | Create Multiple Guest Accounts   |
| create_multi_result<br>Create multiple accounts results page.              | Create Multiple Accounts Results |
| create_user *<br>Create a single guest account.                            | Create New Guest Account         |
| create_user_receipt<br>Create single guest account receipt.                | Create New Guest Account Receipt |
| guest_edit   |                                  |

選擇 visitor\_name (第20行)，然後按一下 Insert After。

## Customize Form Fields (create\_user)

Use this list view to modify the fields of the form **create\_user**.

| Rank | Field                | Type     | Label              | Description   |
|------|----------------------|----------|--------------------|---|
| 1    | enabled              | dropdown | Account Status:    | Select an option for changing the status of this account. |
| 10   | sponsor_name         | text     | Sponsor's Name:    | Name of the person sponsoring this account.               |
| 13   | sponsor_profile_name | text     | Sponsor's Profile: | Profile of the person sponsoring this account.            |
| 15   | sponsor_email        | text     | Sponsor's Email:   | Email of the person sponsoring this account.              |
| 20   | <b>visitor_name</b>  | text     | Guest's Name:      | Name of the guest.  |

Edit
 Edit Base Field
 Remove
 Insert Before
 Insert After
 Disable Field

## Customize Form Field (new)

Use this form to add a new field to the form **create\_user**.

**Form Field Editor**

\* Field Name: username\_auth Select the field definition to attach to the form.

**Form Display Properties**  
 These properties control the user interface displayed for this field.

Field:  Enable this field  
 When checked, the field will be included as part of the form.

\* Rank:   
 Number indicating the relative ordering of user interface fields, which are displayed in order of increasing rank.

\* User Interface: No user interface Revert  
 The kind of user interface element to use when entering or editing this field.

**Form Validation Properties**  
 These properties control how the value of this field is checked.

Field Required:  Field value must be supplied  
 Select this option if the field cannot be omitted or left blank.

Initial Value: 1 Revert  
 Value to initialize this field with when the form is first displayed.

\* Validator: IsValidBool  
 The function used to validate the contents of a field.

Validator Param: (None)  
 Optional name of field whose value will be supplied as the argument to a validator.

Validator Argument:   
 Optional value to supply as the argument to a validator.

Validation Error:   
 The error message to display if the field's value fails validation and the validator does not return an error message directly.

現在建立使用者名稱，以便在AUP訪客門戶頁面後面使用。

導航至CPPM > Guest > Guest > Manage Accounts > Create

— 訪客名稱：訪客WiFi

— 公司名稱：Cisco

— 電子郵件地址：guest@example.com

— 使用者名稱身份驗證：僅允許訪客使用其使用者名稱進行訪問：已啟用

— 帳戶啟用：現在

— 帳戶過期：帳戶不會過期

— 使用條款：我是發起人：已啟用

[Home](#) » [Guest](#) » [Create Account](#)

## Create Guest Account

*New guest account being created by **admin**.*

| Create New Guest Account              |   |
|---------------------------------------|---|
| * Guest's Name:                       | <input type="text" value="GuestWiFi"/><br>Name of the guest.  |
| * Company Name:                       | <input type="text" value="Cisco"/><br>Company name of the guest.  |
| * Email Address:                      | <input type="text" value="guest@example.com"/><br>The guest's email address. This will become their username to log into the network.                                     |
| Username Authentication:              | <input checked="" type="checkbox"/> Allow guest access using their username only<br>Guests will require the login screen setup for username-based authentication as well. |
| Account Activation:                   | <input type="text" value="Now"/><br>Select an option for changing the activation time of this account.  |
| Account Expiration:                   | <input type="text" value="Account will not expire"/><br>Select an option for changing the expiration time of this account.  |
| * Account Role:                       | <input type="text" value="[Guest]"/><br>Role to assign to this account.   |
| Password:                             | <b>281355</b>   |
| Notes:                                | <input type="text"/>  |
| * Terms of Use:                       | <input checked="" type="checkbox"/> I am the sponsor of this account and accept the <a href="#">terms of use</a>  |
| <input type="button" value="Create"/> |   |

建立Web登入表單。導航至CPPM > Guest > Configuration > Web Logins。

名稱：實驗室匿名訪客門戶

頁面名稱：iaccept

供應商設定：Aruba網路

登入方法：伺服器啟動 — 向控制器傳送的授權更改(RFC 3576)

身份驗證：匿名 — 不需要使用者名稱或密碼

匿名使用者：訪客Wifi

條款：要求確認條款和條件

登入標籤：接受並連線

預設URL:[www.example.com](http://www.example.com)

登入延遲：6

更新端點：將使用者的MAC地址標籤為已知端點

高級：自定義與終端一起儲存的屬性，後身份驗證部分中的終端屬性：

使用者名稱 | 使用者名稱

visitor\_name | 訪客姓名

cn | 訪客姓名

visitor\_phone | 訪客電話

電子郵件 | 電子郵件

mail | 電子郵件

保證人名稱 | 發起人姓名

發起人電子郵件 | 發起人電子郵件

Allow-Guest-Internet | true

## 驗證 — 訪客CWA授權

在CPPM中，[導航至Live Monitoring > Access Tracker。](#)

新訪客使用者連線並觸發MAB服務。

「摘要」頁籤：

**Request Details**

Summary Input Output RADIUS CoA

|                        |  |
|------------------------|--|
| Login Status:          | ACCEPT   |
| Session Identifier:    | R0000471a-01-6282a110                            |
| Date and Time:         | May 16, 2022 15:08:00 EDT                        |
| End-Host Identifier:   | d4-3b-04-7a-64-7b (Computer / Windows / Windows) |
| Username:              | d43b047a647b                                     |
| Access Device IP/Port: | 10.85.54.99:73120 (WLC_9800_Branch / Cisco)      |
| Access Device Name:    | wlc01  |
| System Posture Status: | UNKNOWN (100)                                    |

**Policies Used -**

|                        |   |
|------------------------|---|
| Service:               | Guest SSID - GuestPortal - Mac Auth             |
| Authentication Method: | MAC-AUTH  |
| Authentication Source: | None  |
| Authorization Source:  | [Guest User Repository], [Endpoints Repository] |
| Roles:                 | [Employee], [User Authenticated]                |
| Enforcement Profiles:  | Cisco Portal Redirect                           |

◀ ◀ Showing 8 of 1-8 records ▶ ▶ [Change Status](#) [Show Configuration](#) [Export](#) [Show Logs](#) [Close](#)

在同一對話方塊中，導航到選項卡Input。

**Request Details**

Summary Input Output RADIUS CoA

|                        |  |
|------------------------|--|
| Username:              | d43b047a647b                                     |
| End-Host Identifier:   | d4-3b-04-7a-64-7b (Computer / Windows / Windows) |
| Access Device IP/Port: | 10.85.54.99:73120 (WLC_9800_Branch / Cisco)      |

**RADIUS Request**

|                                    |   |
|------------------------------------|---|
| Radius:Airespace:Airespace-Wlan-Id | 4   |
| Radius:Cisco:Cisco-AVPair          | audit-session-id=6336550A00006227CE452457 |
| Radius:Cisco:Cisco-AVPair          | cisco-wlan-ssid=Guest                     |
| Radius:Cisco:Cisco-AVPair          | client-iif-id=1728058392                  |
| Radius:Cisco:Cisco-AVPair          | method=mab                                |
| Radius:Cisco:Cisco-AVPair          | service-type=Call Check                   |
| Radius:Cisco:Cisco-AVPair          | vlan-id=21                                |
| Radius:Cisco:Cisco-AVPair          | wlan-profile-name=WP_Guest                |
| Radius:IETF:Called-Station-Id      | 14-16-9d-df-16-20:Guest                   |
| Radius:IETF:Calling-Station-Id     | d4-3b-04-7a-64-7b                         |

◀ ◀ Showing 8 of 1-8 records ▶ ▶ [Change Status](#) [Show Configuration](#) [Export](#) [Show Logs](#) [Close](#)

在同一對話方塊中，導航到選項卡Output。

## Request Details

Summary Input Output **RADIUS CoA**

|                        |                       |
|------------------------|-----------------------|
| Enforcement Profiles:  | Cisco_Portal_Redirect |
| System Posture Status: | UNKNOWN (100)         |
| Audit Posture Status:  | UNKNOWN (100)         |

### RADIUS Response

|                             |  |
|-----------------------------|--|
| Radius: Cisco: Cisco-AVPair | url-redirect-acl=CAPTIVE_PORTAL_REDIRECT   |
| Radius: Cisco: Cisco-AVPair | url-redirect=https://cppm.example.com/guest/iaccept.php?cmd-login&mac=d4-3b-04-7a-64-7b&switchip=10.85.54.99 |

◀ ◀ Showing 8 of 1-8 records ▶ ▶

Change Status

Show Configuration

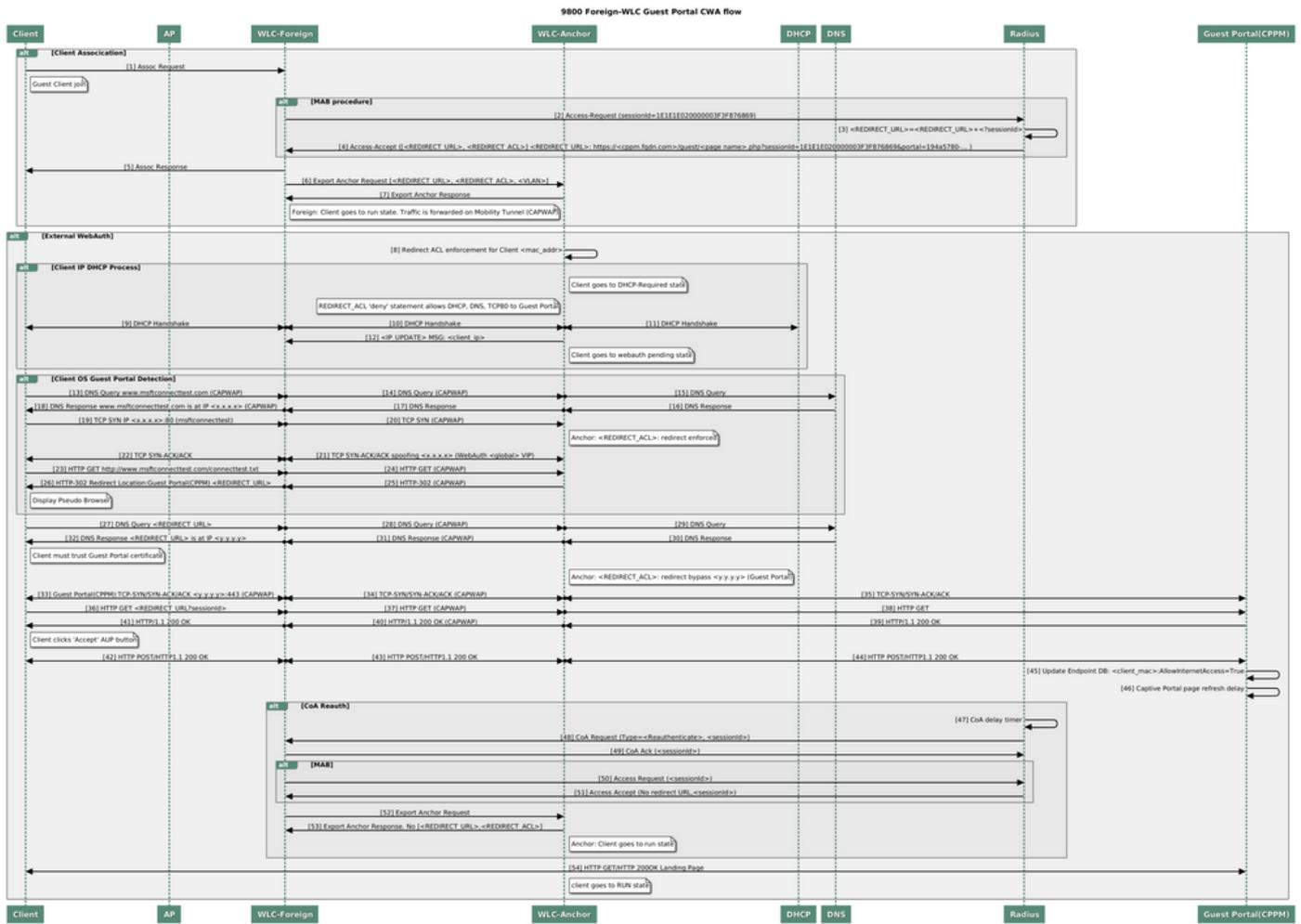
Export

Show Logs

Close

## 附錄

為便於參考，此處提供了思科9800外部、錨點控制器與RADIUS伺服器 and 外部託管訪客門戶互動的狀態流程圖。



使用錨點WLC的訪客中央Web驗證狀態圖表

## 相關資訊

- [思科9800部署最佳實踐指南](#)
- [瞭解 Catalyst 9800 無線控制器設定模型](#)
- [瞭解 Catalyst 9800 無線控制器上的 FlexConnect](#)
- [技術支援與文件 - Cisco Systems](#)

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。